VCX™ Security Guide

VCX™ V7000 IP Telephony Solution
System Release 6.0

Part Number 900-0298-01 AA
Published May 2005

http://www.3com.com/

3Com Corporation
350 Campus Drive
Marlborough, MA
01752-3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hardcopy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with guide.

CONTENTS

ABOUT THIS GUIDE

VCX SYSTEM SECURITY

INDEX

ABOUT THIS GUIDE

This guide describes several issues related to making the VCX V7000 IP Telephony System more secure.

This guide is intended for equipment installers and system administrators who have a thorough understanding of telecommunications, VoIP technology, Linux operating systems, Oracle databases, networks, and system administrator privileges.

If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

`http://www.3com.com/`

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
i	Information note	Information that describes important features or instructions
!	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device
⚡	Warning	Information that alerts you to potential personal injury

Table 2 Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
`Syntax`	The word "syntax" means that you must evaluate the syntax provided and then supply the appropriate values for the placeholders that appear in angle brackets. Example: To enable RIPIP, use the following syntax: `SETDefault !<port> -RIPIP CONTrol = Listen` In this example, you must supply a port number for <port>.
`Commands`	The word "command" means that you must enter the command exactly as shown and then press Return or Enter. Commands appear in bold. Example: To remove the IP address, enter the following command: **`SETDefault !0 -IP NETaddr = 0.0.0.0`**
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in *italics*	Italics are used to: ■ Emphasize a point. ■ Denote a new term at the place where it is defined in the text. ■ Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.

Related Documentation

These 3Com documents contain additional information about the VCX™ V7000 IP Telephony Solution products in this release.

- *VCX Business Telephone Quick Reference Guide*
- *VCX Basic Telephone Quick Reference Guide*
- *V7000 Telephone User Guide*
- *Enterprise Management Suite User Guide*, Version 2.0
- *VCX V7111 Fast Track Installation Guide*
- *VCX V7111 VoIP SIP Gateways User Manual*
- *VCX V7122 Gateway Fast Track Installation Guide*
- *VCX V7122 VoIP SIP Gateways User Manua*l

The following documents are a part of the VCX V7200 IP Call Controller:

- *VCX Installation and Maintenance Guide*
- *VCX Administration Guide*

The following documents are a part of the VCX V7300 IP Telephony Applications Suite:

- *V7350 Unified Messaging Suite Product Overview*
- *V7350 Unified Messaging Suite Installation Guide*
- *V7300 Unified Communications AT - A - GLANCE*
- *V7350 Unified Messaging Suite Operations and System Administration Guide*
- *V7350 Unified Messaging Suite User Guide*
- *V7350 Unified Messaging Suite Intelligent Mirroring Guide*

Your Comments

Your suggestions are important to us because we want to make our documentation more useful to you.

Please send e-mail comments about this guide or any of the 3Com Voice Products documentation and Help systems to:

`VOICE_TECHCOMM_COMMENTS@3com.com`

Please include the following information with your comments:

- Document title
- Document part number (found on the front page)
- Page number
- Your name and organization (optional)

Example:

VCX Installation Guide
Part Number 900-XXXX-01 Rev AA
Page 25

Please address all questions regarding the 3Com software to your authorized 3Com representative.

1 VCX System Security

Overview

VCX V7000 IP Telephony Systems can be configured in a number of ways that enhance system security.

3Com recommends that anyone who is going to configure a VCX system read the latest updates on these items:

- Advisories posted on the CERT/CC (Computer Emergency Response Team/Coordination Center) web site: **www.cert.org**
- The “Top 20” security risk descriptions on the SANS (SysAdmin, Audit, Network, Security) web site: **http://www.sans.org/top20/**
- Notices posted on the CVE (Common Vulnerabilities and Exposures web site: **http://www.cve.mitre.org/**

This chapter contains security-related information on these topics:

Commands

To enhance the security of VCX systems, these commands have been disabled:

- ftp
- telnet
- tftp
- finger
- ident
- rlogin
- rsh
- rcp

To access a VCX system remotely, you must use one of these secure commands:

- ssh
- sftp

The first time that you try to access your VCX system using the ssh or sftp command, you may see a cautionary message asking you to confirm that you want to accept a connection with the VCX system. If you answer yes, the connection is made.

If you completely re-install the VCX system software for any reason, the next time that you try to access the VCX system using the *ssh* or *sftp* command, you may see a warning message that indicates that a "man in the middle" security breach may be in process. This message is the result of new confirmation codes that are generated during the VCX software installation process. If you upgrade from one VCX release to another, no new confirmation codes are generated.

To establish connection to the VCX system:

1. Delete the *known_hosts* file that is referred to in the warning message.
2. Retry the *ssh* or *sftp* command.

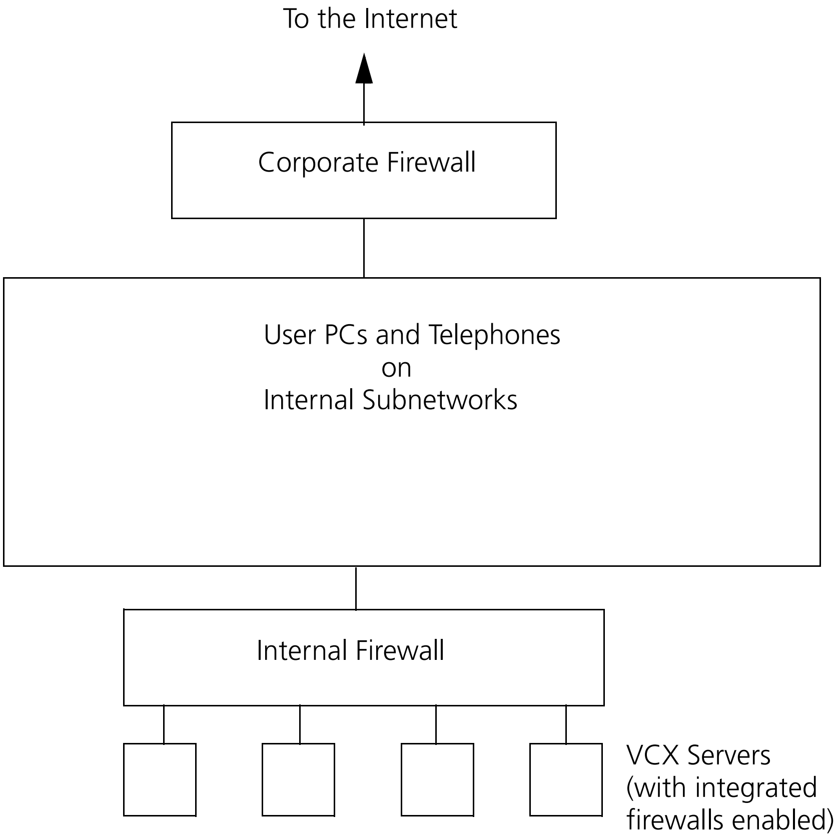
Firewall Configuration

3Com recommends that you:

- Isolate your VCX system from the Internet by configuring it behind your corporate firewall
- Isolate your VCX system from computers inside your company by configuring it on a separate subnetwork or placing it behind an internal firewall
- Always leave the integrated firewall enabled on each VCX server.

Example Network Configuration

This network diagram illustrates one way to isolate the VCX system.


To the Internet
Corporate Firewall
User PCs and Telephones on Internal Subnetworks
Internal Firewall
VCX Servers (with integrated firewalls enabled)

TCP Port Access

Use the information in this section to configure your internal firewall. The VCX system allows remote network access to these TCP ports:

Port Number	Port Type	Service Requiring the Port
22	TCP	SSH
53	UDP	DNS
80	TCP	HTTP
123	UDP	NTP
161	UDP	SNMP
443	TCP	HTTPS
2093	UDP	SIP downloader
5060	UDP	SIP
5065	UDP	SIP

Note: Port 5065 is used only on a branch office server that:

- Uses only the eth0 network interface
- Runs the IP Telephony and Messaging software configuration

Back End Server Ports

The Back End Servers (Accounting Server, Authentication and Directory Server) use these ports in order to provide redundant service to remote clients. Normally, these ports can be blocked by the internal firewall. However, if the redundant servers are separated on either side of the internal firewall, the firewall must be configured to *not* block these ports.

Port Value	Service Requiring the Port
1521	Oracle Listener Service
1645	3Com Authentication Server (RADIUS)
1646	3Com Accounting Server (RADIUS)
1781	3Com Accounting Server (3Q)
1783	3Com Directory Server (3Q)
1784	3Com Authentication Server (3Q)
1786	3Com Accounting Server (3Q)
1788	3Com Directory Server (3Q)
1789	3Com Authentication Server (3Q)
38000	Global Directory Server (used between multiple regions and between regions and branches)

RTP Port Range Calculations

To calculate the highest RTP port number used by the VCX Unified Messaging Suite, use this formula:

Highest Port Number = (Number of Ports) * 2 + (Start RTP Port -1)

Formula Element	Explanation
Number of Ports	The default for IP Messaging is 144 ports. During the IP Messaging installation process, you are given an opportunity to change this value. If you changed the value, use the number that you chose. Add the number of ports used by the V7111 and V7122 gateways on your system. See "Analog and Digital Gateway Ports", later in this section.
Start RTP Port	Default = 8000. If you have modified the default starting port number, use the number you selected.

UDP Port Range Calculations

The IP Messaging System transmits and receives fax information using the UDPTL protocol and uses UDP ports. UDP port numbers start immediately after the RTP port range.

Starting UDP Port Number

To calculate the starting port number in the UDP range, use this formula:

UDP Start Port = (Number of Ports) * 2 + (Start RTP Port)

Formula Element	Explanation
Number of Ports	The default for IP Messaging is 144 ports. During the IP Messaging installation process, you are given an opportunity to change this value. If you changed the value, use the number that you chose. Add the number of ports used by the V7111 and V7122 gateways on your system. See "Analog and Digital Gateway Ports", later in this section.
Start RTP Port	See "RTP Port Range Calculations", earlier in this document.

Ending UDP Port Number

To calculate the ending port number in the UDP range, use this formula:

UDP ending port number = (UDP Start Port) +(Number of Ports -1)

Formula Element	Explanation
UDP Start Port	See the calculation in "Starting UDP Port Number", earlier in this section.
Number of Ports	The default for IP Messaging is 144 ports. During the IP Messaging installation process, you are given an opportunity to change this value. If you changed the value, use the number that you chose. Add the number of ports used by the V7111 and V7122 gateways on your system. See "Analog and Digital Gateway Ports", later in this section.

Analog and Digital Gateway Ports

The VCX system includes V7111 Analog Gateways for connection to the Public Swithced Telephone Network (PSTN) through analog phone lines or to analog telephones and fax machines. It also uses digital gateways to connect to the PSTN (T1 and E1 spans).

The V7111 Analog Gateways use these ports:

Table 1 V7111 Analog Gateway Port Numbers

Channel Number	UDP Port	T.38 Port (fax)
1	4000	4002
2	4010	4012
3	4020	4022
4	4030	4032
5	4040	4042
6	4050	4052
7	4060	4062
8	4070	4072
9	4080	4082
10	4090	4092
11	4100	4102
12	4110	4112
13	4120	4122
14	4130	4132

Table 1 V7111 Analog Gateway Port Numbers (continued)

Channel Number	UDP Port	T.38 Port (fax)
15	4140	4142
16	4150	4152
17	4160	4162
18	4170	4172
19	4180	4182
20	4190	4192
21	4200	4202
22	4210	4212
23	4220	4222
24	4230	4232

The V7122 Digital Gateways use these port numbers:

Table 2 V7122 Digital Gateway Port Numbers

Channel Number	UDP Port	T.38 Port (fax)
General Formula: (n = channel number)	6000+10(n-1)	6002+10(n-1)
Examples: This table includes only sample channel numbers. Use the general formula to calculate port numbers for channel numbers that are not shown.		
1	6000	6002
2	6010	6012
3	6020	6022
4	6030	6032
5	6040	6042
6	6050	6052
7	6060	6062
8	6070	6072
96	6950	6952
120	7190	7192
192	7910	7912
240	8390	8392
384	9830	9832
480	10790	10792

IP Messaging Ports

The IP Messaging System (vcxums) uses these ports. If your VCX system does not use IP Messaging, the integrated firewall on each VCX server will disable access to these ports.

Port Number	Port Type	Service Requiring the Port
25	TCP	SMTP
110	TCP	POP3
143	TCP	IMAP
389	TCP	LDAP

Passwords

VCX systems that are shipped from 3Com have default passwords configured for system-level login IDs.

3Com strongly recommends that you change the passwords for these login IDs:

- app
- cworks
- root
- vcx
- oracle
- tomcat

3Com recommends that you secure the new passwords in a manner consistent with your company's security guidelines.

SIP Invite Messages

3Com recommends that you configure the Call Processor to challenge all SIP invite messages.

To configure this capability using a remoteCli command:

1. Start the remoteCli process by entering these commands.

```
cd /opt/3com/VCX/callprocessor/remoteCli/bin
./remoteCli -call
```

2. After remoteCli starts, enter this command.

```
>config CcCfg ChallengeAllCalls=true
```

To configure this capability using the Enterprise Management Suite:

1. For each VCX server, locate the Configuration tab for the SIP call process.
2. Set the "ChallengeAllCalls” value to "true."

SNMP

The VCX system supports version v1 of the Simple Network Management Protocol (SNMP). SNMP v1 passes community names in clear-text. 3Com advises that you restrict SNMP access to VCX servers using one of these methods:

- Permit only hosts on trusted subnets to access the VCX servers.
- Use the Enterprise Management Suite (EMS) to configure each VCX server and restrict access to authorized work stations only.

To restrict access to a VCX server using EMS:

1. In the EMS Explorer pane on the left, select the VCX server that you want.
2. For each work station that you want to have access to the VCX server, in the right pane, select *Authorized Stations* > *Add.*
3. Enter the IP address and network mask for the authorized station.

Both the EMS and VCX SNMP agent comply with CERT advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP).

Voice Mail Access

If any of the VCX system users access their voice mail from PCs using a POP3 client, the login IDs and passwords that they use are transmitted over the network with no encryption.

INDEX